Tokyo Hackathon Challenges from Cybex

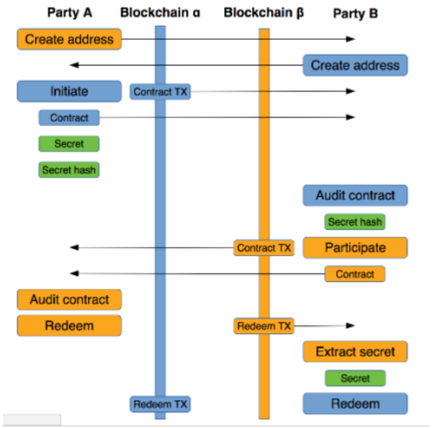
Background

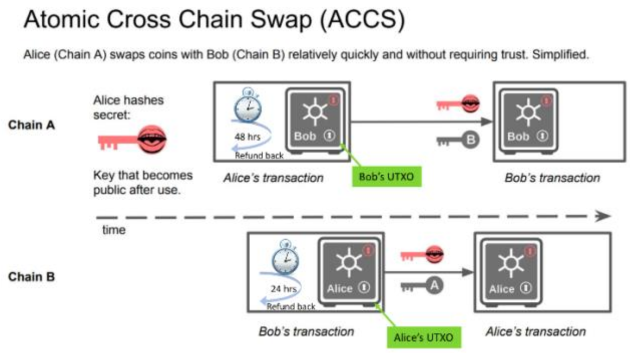
Atomic Swap in CYBEX

Atomic swaps between CYBEX and Bitcoin involve each party paying into a locked account. In the case of CYBEX, it’s a multi-signature account; in the case of Bitcoin, it’s an UTXO with a scripted lock. The creator of Litecoin, Charlie Lee, successfully implemented and demonstrated atomic swaps using Litecoin in exchange for Bitcoin, Vertcoin and Decred. However, this type of swap only works between the Bitcoin-like chains with similar scripting systems as well as support for CLTV (Check Lock Time Verify) functionality.

https://github.com/decred/atomicswap

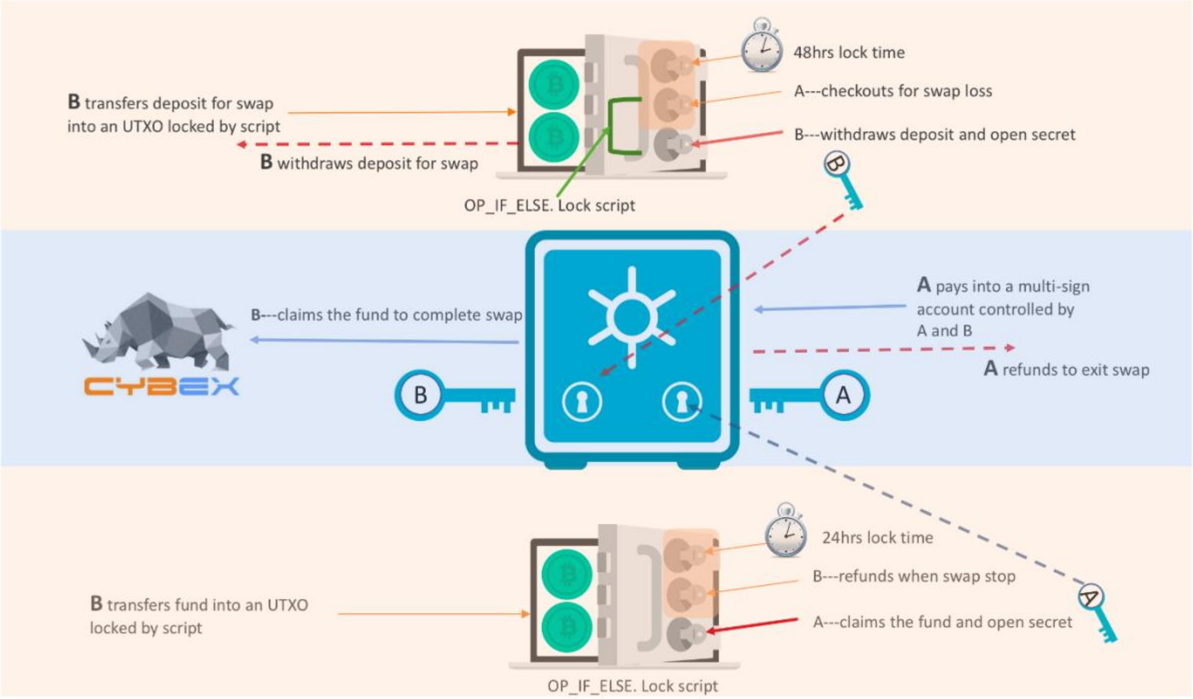
With CLTV script, lock time windows can be set for the refund operation, the initiator sets 48 hours lock time for the participator to pay and redemption, the participator sets 24 hours lock time for the initiator to redemption. This time-locked refund scheme guarantees the atomic integrity that any party can withdraw his fund completely when the other party quits the swap process.





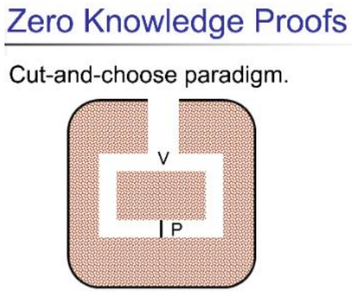
But since CYBEX doesn’t have the Bitcoin-like scripting system, we use a multi-signature account to lock the CYB that the initiator pays to participator (assuming that the initiator pays CYB) and using the script to lock Bitcoin that participator pays to initiator in UTXO.

One drawback is that the multi-signature method cannot implement a recovery and refund process, CYBEX resolves this with a requested deposit to incentivize and guarantee the trade’s integrity.


48hrs lock time
B transfers deposit for swap into an UTXO locked by script
A---checkouts for swap loss
B---withdraws deposit and open secret
B withdraws deposit for swap
OP_IF_ELSE. Lock script
B
A pays into a multi-sign account controlled by A and B
B---claims the fund to complete swap
CYBEX
A refunds to exit swap
B
A
24hrs lock time
B---refunds when swap stop
B transfers fund into an UTXO locked by script
A---claims the fund and open secret
A
OP_IF_ELSE. Lock script

Atomic swap between CYBEX and Bitcoin

In CYBEX, an atomic swap begins with a cut and choose game for public key and key hash exchange



Start of atomic swap in CYBEX

Through a batch of interactions, both parties will have the other’s temporary public key and a hash of key with high probability proof that they are generated from the same private key. Then the public key and hash of private key will be used in the Bitcoin script to verify the redemption.

https://bitcointalk.org/index.php?topic=1340621.msg13828271#msg13828271

Challenge : Using Vesting Balance in Cybex to implement the functions of CLTV in Bitcoin

Because CYBEX requests deposit to incentivize and guarantee the trade's integrity, further large tx memo size necessary for cut and choose algorithm, so the atomic swap prototyping above is just suited to large amount crypto-currency swap between two recognized party.

Can you use Vesting Balance of Cybex to implement the similar function of CLTV in Bitcoin to simplify to the swap model. You can refer the below

https://github.com/bitshares/bitshares-core/blob/416f058abd52720668f1bc1c9717fd57e284e44d/testnet-shared-vesting-balances.txt

https://github.com/bitshares/bitshares-core/blob/416f058abd52720668f1bc1c9717fd57e284e44d/libraries/chain/include/graphene/chain/protocol/vesting.hpp